



National Infrastructure Protection Center NIPC Daily Open Source Report for 10 January 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports the U.S. is urging countries that export oil to increase production, due to the worldwide shortage caused by the political problems in Venezuela and the possibility of war with Iraq. (See item [2](#))
- Platts Energy News reports the Nuclear Regulatory Commission has called for additional security enhancements to close a potential security gap. (See item [3](#))
- eSecurity Planet reports two major viruses have struck the Internet at the same time: W32.Lirva.A and ExploreZip. (See item [21](#))
- The Associated Press reports Organization of American States officials are considering ways to cooperate in preventing terrorists from operating in the Caribbean or using it as a way-station for attacks on the United States. (See item [23](#))

NIPC Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [NIPC Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 09, Associated Press* — Powder stolen from Kyrgyzstan plant. Masked men armed with clubs forced their way into a once-secret chemical plant in Kyrgyzstan and stole 1,000 pounds of europium oxide, a powder that can be used in nuclear reactors, police said Thursday. The attackers beat, tied up and disarmed two guards at the plant in Orlovka, 50 miles northeast of the capital Bishkek, before dawn on Wednesday. They then cut the locks on a storage area and fled with 23 44-pound containers of the material, the Interior Ministry press

service said. In the Soviet era, the installation in Orlovka was secret. **Among other uses, Europium oxide can be used to make the rods that control nuclear reactions.** It is not radioactive, however.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A32352-2003Jan9.htm> 1 :

2. *January 09, New York Times* — **U.S. lobbies oil exporters to produce more.** The Bush administration, alarmed by a 38-day strike that has crippled Venezuela's petroleum industry and caused sharp increases in prices, has begun pressing countries that export oil to increase production, administration officials said today. Those efforts, which are being led by senior officials in the State and Energy Departments, also seem intended to prepare for the potential disruption in the international oil market that would come from an invasion of Iraq, industry analysts said. The globe-spanning lobbying campaign could bear fruit this weekend, when the Organization of the Petroleum Exporting Countries (OPEC) is expected to meet in Vienna **to discuss increasing production as much as two million barrels a day, or 8.7 percent. Venezuela has been the fourth-largest source of oil for the United States, behind Saudi Arabia, Mexico and Canada, providing 14 percent of the nation's crude oil imports.** By some estimates, Venezuelan production has fallen 75 percent or more since a general strike, organized by opponents of President Hugo Chávez, began last month. **"We were consuming 1.5 million barrels of Venezuelan oil each day that we're not getting now, which means we have to get it from someplace else,"** a senior State Department official said. "We've had a historic strategic energy relationship with Venezuela that is obviously being affected in a dramatic way at this point."

Source: <http://www.nytimes.com/2003/01/09/business/09OIL.html>

3. *January 08, Platts Energy News* — **NRC tells nuclear plant operators to tighten security.** The US Nuclear Regulatory Commission (NRC) Wednesday ordered operators of 103 operating nuclear plants to close what had been criticized as a potential security gap. The orders both formalize a series of security measures plant operators had taken in response to the Sep 11, 2001, terrorist attacks and calls for additional security enhancements to address potential problems identified in comprehensive security reviews. Although the agency would not disclose details of the orders, **it said the measures generally include restricting temporary unescorted access to a plant and re-verifying background investigations for those individuals with unescorted access.** The order also requires plant operators to share critical background investigations with other operators.

Source: <http://www.platts.com/stories/nuclear4.html>

4. *January 08, Richmond Times-Dispatch* — **Pennsylvania group tries to assure Virginia lawmakers of utilities' takeover.** A Pennsylvania-based organization sought to assure state lawmakers yesterday that consumers will not be harmed if it takes over the power lines of Virginia's two largest utilities. Steven Herling is the top system planner for PJM Interconnection, which operates power lines and regional power markets in parts of seven states and the District of Columbia. **Dominion Virginia Power and American Electric Power (AEP), which serve a combined 2.6 million Virginia customers, have announced plans to turn over operation of their transmission lines to PJM.** While AEP recently accelerated its plans to join PJM, Dominion delayed its application to join after lawmakers and others raised concerns that Virginians could be hurt by the move. Dominion, however, said the delay still might not keep it from joining PJM by a planned Oct. 1 entry date. Herling said PJM would

never force Virginians to cut back on power use so that electricity could be shipped to other states, as some fear. **Lawmakers quizzed him about concerns that the state could lose the ability to make sure the two utilities' power systems are operated to the benefit of Virginians if they join multistate PJM.** Joining would put the utilities under the jurisdiction of federal regulators. Herling responded that the conflict between state and federal jurisdiction is not his group's concern.

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3557193

[\[Return to top\]](#)

Chemical Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *January 09, Congressional Budget Office* — **The long-term implications of current defense plans.** The Defense Subcommittee of the Senate Appropriations Committee asked the Congressional Budget Office (CBO) to produce annual projections through 2020 of the resources that might be needed to carry out the Administration's plans for DoD. CBO has also examined the implications of those plans for quantities and ages of major weapon systems. Carrying out the plans in the 2003 FYDP would require DoD to spend an average of \$426 billion a year (in 2002 dollars) between 2008 and 2014 and \$430 billion a year from 2015 to 2020, CBO projects. Those figures, however, are based on DoD's cost estimates, which have frequently been underestimated. **If costs for operations and investment grew as they have in the past, carrying out the Administration's plans would require spending an average of \$464 billion a year between 2008 and 2014 and \$480 billion per year from 2015 to 2020.** In either case, future resource demands would be higher than defense spending has been at any time since 1980—and would need to remain at those higher levels for a decade or more. **Viewed in relation to the size of the economy, however, future demand for defense resources could be lower than past spending. DoD's share of the budget dropped from an average of 28 percent in the 1980s to 18 percent in 2002. If the rest of the budget continued to grow as CBO currently projects, defense spending would fall to about 13 percent of the total budget by 2020. The share of the nation's gross domestic product (GDP) allocated to defense would also drop from an average of 6 percent in the 1980s to about 2 percent by 2020 (assuming that GDP grew at the rates projected by CBO)—or half the share of GDP devoted to defense in the 1990s.** If DoD received enough funding to carry out its current plans through 2020 (as CBO projects them), it would succeed in halting or reversing the aging trends that have been developing since the late 1990s for many types of weapons. In addition, if recently begun programs associated with military transformation proved successful, DoD might be able to reduce its long-term procurement needs by 10 percent to 15 percent, CBO estimates. **But given the long time periods associated with developing and fielding new military equipment, transformation programs started now would be unlikely to provide substantial operational capabilities for many years.**

Source: <http://www.cbo.gov/execsum.cfm?index=4010Sum.htm>

6. *January 09, Inside the Pentagon* — **DOD transfers funds to Homeland Security Dept. to study bioweapons.** The Defense Department will transfer \$420 million this year from its chemical and biological defense program to the Department of Homeland Security so the new agency can spearhead its own projects to benefit civilians. **On Dec. 18, the Pentagon comptroller moved the fiscal year 2003 dollars from the Defense Threat Reduction Agency, which oversees the military's chem-bio defense program, to DHS. A Pentagon spokesman said the new federal agency is expected to use the money to establish a "National Bio-Weapons Defense Analysis Center" and pursue efforts to detect biological agents in urban areas.** The transfer in funds does not, however, indicate a diminished role for the military in chem-bio defense. Defense Secretary Donald Rumsfeld requested the amount on top of his \$1 billion FY-03 request for such programs, promising lawmakers the military would relinquish the \$420 million to the homeland security agency when needed.

Source: <http://ebird.dtic.mil/Jan2003/s20030109144991.html>

7. *January 08, U.S. Army Tank-Automotive and Armaments Command* — **Army's new SmarTruck vehicle adapts to counterterrorism and homeland security missions.** The Army Tank-automotive and Armaments Command's National Automotive Center (NAC) today unveiled SmarTruck II, a versatile prototype, multi-purpose vehicle capable of both counterterrorism support and homeland security for a variety of community service and humanitarian aid missions. **Built on a modified Chevrolet Silverado platform, this innovative 6x6 all-wheel drive vehicle is engineered to meet military, homeland security, counterterrorism and municipal government challenges in a post-Sept. 11 environment. SmarTruck II packs a bevy of electronically intelligent devices, state-of-the-art global communication systems and weapon options that will give its crew some crucial mission advantages.** "SmarTruck II is a multi-purpose vehicle for what are, in reality, 'multi-purpose' missions. This unique vehicle is now ready and able to meet those challenges facing local, state and federal agencies," said Dennis J. Wend, executive director of the NAC. "If you don't know exactly what you need, what's the next best thing? A modular vehicle that can become anything you want it to be." SmarTruck II incorporates an interchangeable mobile applications system.

Source: http://www.techmarketing.brtrc.com/webdev/nac/site/media_rls_2003_0107.htm

[[Return to top](#)]

Banking and Finance Sector

Nothing to report.

[[Return to top](#)]

Transportation Sector

8. *January 09, Washington Post* — **Passengers paid far more than airlines for security. Airline passengers paid the federal government nearly \$1 billion for security last year, more than six times the amount the airline industry paid, according to the agency in charge of airport security.** Both passengers and airlines were required by Congress after the terrorist attacks in 2001 to help pay for security. But passengers have paid far more and airlines far less than the government first predicted. **Passengers paid \$977 million in the fiscal year that**

ended in September, through \$2.50 security fees that have been added to airline ticket prices for each segment of a flight since last January, the Transportation Security Administration said. **During the same period, airlines paid \$160 million, although the industry did not begin making payments until midway through the fiscal year.** This fiscal year, the TSA expects airlines to pay \$318 million for security, according to congressional and industry sources.
Source: <http://www.washingtonpost.com/wp-dyn/articles/A30178-2003Jan8.htm>

[[Return to top](#)]

Postal and Shipping Sector

9. *January 09, Business Wire* — **Smart and Secure Tradelanes ships first 100 "Smart Containers" across Pacific Ocean with real-time tracking and detection.** The first wave of "smart and secure" ocean containers filled with merchandise to replenish store shelves for the New Year have been transported over the Pacific Ocean between major ports in Asia and the U.S. West Coast. **These milestone shipments mark the successful operational deployment of Smart and Secure Tradelanes, the world's largest public-private initiative to improve the end-to-end security and efficiency of container transportation.** This unique partnership is sponsored by the Strategic Council on Security Technology, a global advisory resource and catalyst for cargo and includes a rapidly growing list of partners, including major shippers, port and terminal operators, transportation service providers and technology solution providers. **The groundbreaking SST initiative repurposes infrastructure, processes, and technology used by the U.S. Department of Defense to deliver both productivity and security benefits to ports, terminal operators, service providers, carriers, and shippers.** By leveraging existing proven methods within the context of an open system which allows for innovation and expansion, SST has created a solid baseline infrastructure that vastly improves security and productivity now and can be enhanced over time as new technologies and enhanced processes are deployed. **Over the past month, SST partners have shipped more than 100 40-foot long ocean containers, which have been equipped with electronic seals that detect security breaches and instantly communicate their status and location over radio frequencies to a web-based software security network.** The first 100 of these "smart and secure" containers have been shipped between the ports of Hong Kong, Singapore, Seattle and Los Angeles and Long Beach over the past six weeks.
Source: http://biz.yahoo.com/bw/030109/90178_1.html

10. *January 08, U.S. Customs Service* — **Spain signs declaration of principles to join U.S. Customs Container Security Initiative.** U.S. Customs Commissioner Robert C. Bonner and Nicolas Bonilla Penvela, the Spanish Director General of Customs today announced that the government of Spain has agreed to participate in the U.S. Customs Container Security Initiative (CSI). CSI is a U.S. Customs initiative designed to prevent the smuggling of terrorists or terrorist weapons in ocean-going cargo containers. **Under terms of the declaration announced today, U.S. Customs officers will be stationed at the port of Algeciras.** "I applaud the government of Spain for their strong support in helping to make a safer, more secure world trading system," said Commissioner Bonner. "CSI is an insurance policy against terrorism. In signing this declaration of principles today, the government of Spain has taken an important step. CSI will help secure trade moving between the ports of Spain, and the ports of the United States, and it will do so without slowing down trade." One

element of CSI involves placing U.S. Customs inspectors at foreign seaports to target and pre-screen U.S.-bound cargo containers before they are shipped to America. **"We are looking to expand CSI beyond the top 20 ports, as rapidly as we can. Once we have implemented CSI at most of the top 20 ports, we will quickly expand CSI to all ports that ship substantial amounts of cargo to the United States, and that have the infrastructure and technology in place to participate in the program,"** Commissioner Bonner said.

Source: <http://www.customs.ustreas.gov/hot-new/pressrel/2002/01082003-00.htm>

[\[Return to top\]](#)

Agriculture Sector

11. *January 09, United Press International* — **Newcastle quarantine extended in Southern California. Agriculture officials extended the quarantine against chickens that might be afflicted with Exotic Newcastle disease to eight Southern California counties Wednesday while officials in Washington state asked that its residents be on the lookout for signs the disease was spreading to other western states.** More than 1 million chickens have been destroyed since Exotic Newcastle was discovered on a commercial egg farm in December. At the time, Los Angeles, San Bernardino, Riverside, and San Diego Counties were placed under quarantine. The U.S. Department of Agriculture (USDA) added Santa Barbara, Imperial, Orange and Ventura Counties to the list late Wednesday as a precaution against the disease spreading farther. **"The expanded quarantine creates a buffer zone around infected sites and provides additional security against spread of the disease,"** the USDA said in a release. **"To do this, additional quarantines are immediately being imposed on non-infected counties adjacent to those counties infected with disease through the declaration of extraordinary emergency issued by the USDA today."**

Source: <http://www.upi.com/view.cfm?StoryID=20030109-013109-6188r>

12. *January 09, Reuters* — **Rocky Mountain Park to test deer for deadly disease. Rocky Mountain National Park said it will conduct a major research program to test each of its 500 mule deer for a fatal brain sickness related to "mad cow disease.** Five percent of the Colorado park's mule deer population is believed to be infected with chronic wasting disease (CWD) a once obscure fatal illness in which misshapen proteins called prions cause the brains of deer or elk to waste away. Research has shown the disease could cause a decline in deer herds if more than 5 percent of the animals contract it. "It's a live test, which is uniform with the park's goal of eliminating a disease, but keeping the deer that are healthy," park spokeswoman Kyle Patterson said. **The deer testing, which will continue through 2005, is scheduled to begin on Jan. 21. Animals found with the disease will be killed because the disease is highly contagious.**

Source: http://www.enn.com/news/wire-stories/2003/01/01092003/reu_49315.a.sp

[\[Return to top\]](#)

Food Sector

13.

January 09, Food Production Daily — **Opinion call for SRM changes. The United Kingdom Food Standards Agency is seeking views on proposed changes to EU regulations that will extend the list of animal tissues that are regarded as specified risk material (SRM) and banned from entering the food chain.** SRM controls are among the key measures used to ensure Bovine Spongiform Encephalitis (BSE) infectivity does not enter the food supply. They are also applied to some sheep and goat tissue as a precautionary measure because of the possible risk that BSE may exist in sheep and goats. **The proposed EU measures would extend the current list of SRMs to include the ileum of sheep and goats of all ages and the tonsils of cattle of all ages.** The amended regulations would also require that bovine tongue would have to be removed in a certain way, so as to ensure that there is no risk of visible tonsil tissue on the tongue.

Source: <http://www.foodproductiondaily.com/news/news.asp?id=1979#>

[\[Return to top\]](#)

Water Sector

14. *January 09, Water Tech Online* — **Water infrastructure funding bill introduced in Congress. U.S. Representatives Sue Kelly, R-NY, and Ellen O. Tauscher, D-CA, this week introduced in the House of Representatives a bipartisan Clean Water Infrastructure Financing Act of 2003 (HR 20), which would provide \$25 billion over five years for the state revolving fund used for much-needed water and wastewater infrastructure upgrade and rehabilitation.** In a report, the Water Infrastructure Network (WIN) said a \$12 billion annual shortfall exists for wastewater infrastructure over the next twenty years. These estimates have been bolstered by the US Environmental Protection Agency, the Government Accounting Office, and the Congressional Budget Office.

Source: <http://www.watertechonline.com/news.asp?mode=4font>>

[\[Return to top\]](#)

Public Health Sector

15. *January 09, Canton Repository* — **Health officials seek more money to fight bioterrorism. Eight of 10 local public health departments feel better prepared to handle a bioterrorism attack than they did a year ago, thanks to more than \$1 billion in federal aid, a national survey found.** The agencies, however, still don't feel fully prepared, the December tally of 500 health departments revealed. The National Association of Counties (NACO) and the National Association of County and City Health Officials sponsored the telephone survey conducted by National Research. NACO lobbies the federal government to adopt policies and provide funding that benefit local government. **The survey revealed that 84 percent of responding health departments believe they are better prepared to respond to biological attack than a year before. In a survey last January, more than 90 percent of respondents said they were unprepared for bioterrorism.**

Source: <http://www.cantonrep.com/index.php?ID=79580/a>>

16.

January 09, National Post — **Law to require doctors to report West Nile. Doctors in Ontario, Canada who suspect a patient has West Nile virus will soon be legally required to report their diagnosis to the local medical officer of health. The measure is part of the province's plan to be ready for the start of mosquito season this spring, when it is expected there will be a rise in the number of humans infected with the disease. Ontario's aggressive strategy is likely the start of a national trend as the federal government and other provinces gear up for the spread of the disease throughout many parts of the country. In Ontario, said Dr. D'Cunha, there were 119 confirmed cases and 192 probable cases of West Nile in humans last year. There has been one confirmed death in the province, but the fatality tally might be as high as eight. Coroners in some cases have not yet ruled whether people with West Nile actually died from the virus or from other causes. In any event, Dr. D'Cunha said the province wants to be prepared for the start of mosquito season. He revealed that among the measures to be taken is making West Nile a reportable disease.**

Source: <http://www.nationalpost.com/national/story.html?id=%7B2A1E48B6-3003-42F5-9442-5ACB76B5641F%7D>

[\[Return to top\]](#)

Government Sector

17. *January 09, Washington Post* — **Agencies moving to Homeland Security could be hit hard by retirements.** Six major agencies moving into the Department of Homeland Security could lose roughly a quarter to half of their staffs to retirement in the next five years, according to data collected by the Partnership for Public Service. **The data show that about twice as many employees at the six agencies will be eligible to retire by the end of 2008 than are currently eligible. Overall, 26,363 employees out of 67,166 at the six agencies would be eligible to retire in 2008, according to the snapshot taken in 2001, the latest data available. Max Stier, the partnership's president, said the Department of Homeland Security could face a "one-two punch" if it follows private-sector trends. A survey by Watson Wyatt consultants found that 47 percent of company executives depart in the first year of a corporate merger and 75 percent leave in the first three years, Stier said. Retirement scenarios are based on moving targets, to some degree. The percentage of retirement eligibles in 2008 can change if more or fewer employees leave between now and then. In the past, relatively few employees have retired in the year they became eligible. Given the slumping economy, administration officials think employees will be staying on the federal payroll longer rather than depending on retirement savings and pensions.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A30830-2003Jan8.htm>

18. *January 09, Washington Post* — **Cox to head new Homeland Security panel.** Rep. Christopher Cox, a senior member of the House GOP leadership, will head the newly created homeland security committee, House Speaker Dennis Hastert said Wednesday. **The California conservative will be the first chairman of the panel responsible for overseeing the giant new Homeland Security Department that President Bush signed into law late last year. Cox, 50, was first elected to Congress in 1988 and has been the head of the House Republican Policy Committee since the Republicans captured control of the House in 1995. House Democratic leader Nancy Pelosi, D-Calif., will name the top Democrat on the "select" committee, which will differ from other "standing" committees in that it will focus on**

specific oversight or investigative functions.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A30721-2003Jan8.htm> 1

19. *January 09, Richmond Times-Dispatch* — **Proof of legal status said no safety boost.** Virginia shouldn't change the law to make people prove they are in the United States legally to receive a driver's license or state photo ID card, according to a state study released yesterday. **The Department of Motor Vehicles concluded that the requirement would not make Virginians any safer from terrorism and would cost more than \$5.5 million a year to carry out at a time when the agency has been laying off employees and shuttering offices to save money. However, the study called for legislation that would allow Virginia to begin collecting biometric information, such as fingerprints or retinal scans, that would become part of the license.**

Source: <http://www.timesdispatch.com/news/politics/MGBIME73QAD.html>

[[Return to top](#)]

Emergency Services Sector

Nothing to report.

[[Return to top](#)]

Information and Telecommunications Sector

20. *January 09, Federal Computer News* — **Council offers vision for infosec standards.**

President Bush's private-sector infrastructure protection advisory council agreed January 8 that **the federal government should encourage the development and use of open standards in the market instead of dictating specific standards. But federal officials should also use the government's significant buying power to push for interoperability in those market standards and solutions that will raise the baseline of security across all sectors. The National Infrastructure Advisory Council's report will go to the president later this month** along with a revised National Strategy to Secure Cyberspace, said Richard Clarke, chairman of the President's Critical Infrastructure Protection Board. The recommendations fall in line with the approach taken by the Bush administration in its draft cybersecurity strategy, which the White House released in September 2002 for comment. Revisions proposed by Clarke's office include setting specific priorities, such as taking a closer look at the Common Criteria security product certification program. Later this month, the council plans to meet again to look at **other infrastructure protection issues, including the international migration to Version 6 of the Internet Protocol and developing a systematic vulnerability assessment program for private-sector infrastructure.**

Source: <http://www.fcw.com/fcw/articles/2003/0106/web-niac-01-09-03.asp>

21. *January 09, eSecurity Planet* — **Virus Alert: W32.Lirva.A and ExploreZip.** Two major viruses have struck the Internet at the same time. **ExploreZip, an Internet worm first let loose in the wild back in 1999, has reemerged with just enough changes made to allow it to slip through anti-virus software undetected.** And it has the added ability to override files on the infected computer, as well as on any other computer in the same network. **Once ExploreZip**

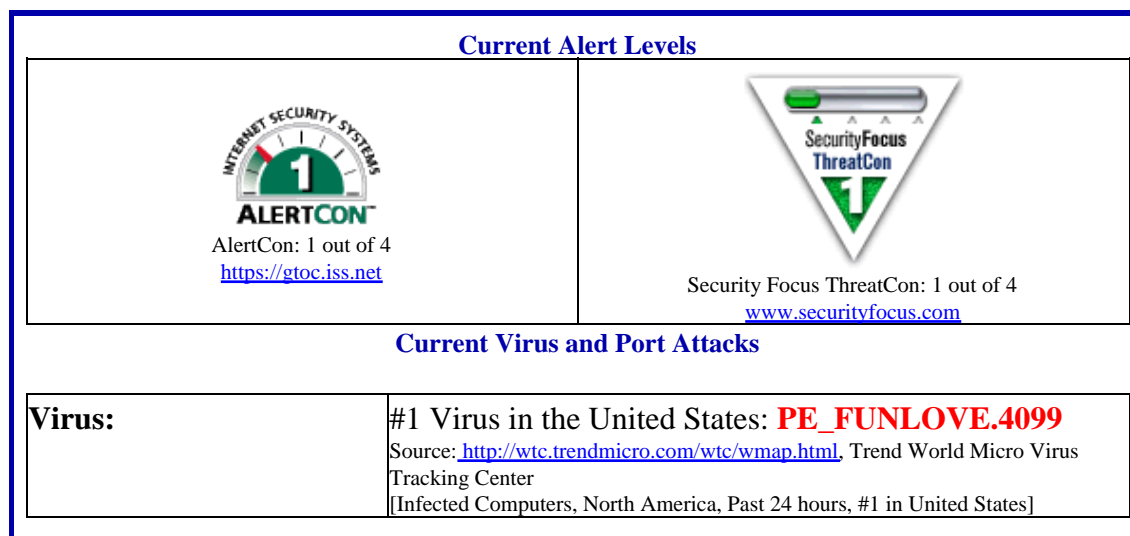
infects a computer, it will automatically respond to any email received with a seemingly valid subject line and the user's name, along with an infected attachment. Another problematic virus is the mass-mailing worm that pays tribute to Canadian singer Avril Lavigne. **The worm is going under a few different names, including Avril and Lirva (which is Avril spelled backwards).** Although this virus is less destructive than ExploreZip, anti-virus software company F-Secure Corp. has rated both viruses as Level 2 Threats, the second-highest threat category. The Lirva worm got a Level 2 rating because of the speed with which it's spreading around the world. It reportedly originated, in middle Europe and has spread to Turkey, the United States and Southeast Asia in less than 48 hours. **Once Lirva infects a computer, it opens the computer's Internet Explorer browser to official Avril Lavigne Web site on the 7th, 11th and 24th of the month. It then starts to display colored circles on the screen, freezing the computer.**

Source: http://www.esecurityplanet.com/trends/article/0..10751_1567161.00.html

22. *January 09, Government Computer News* — **DOD says system pilot not affected by TriWest thefts. The December 14 theft of computer equipment containing information on more than 500,000 military members poses no threat to the Composite Health Care System II, the Defense Department's pilot computerized medical system still in development, a Defense health official said yesterday. The computers were stolen from a TriWest Healthcare Alliance office in Phoenix. TriWest provides managed health care to 1.1 million military personnel and their families in 16 states for DOD's health care service, known as the Tricare Management Activity. But Tricare is not part of CHCS II, the official said. "There is no relationship between those two (systems)," said Dr. William Winkenwerder, Jr., assistant secretary of Defense for health affairs. Furthermore, Winkenwerder said, CHCS II information is stored at "very secure sites" and that DOD had implemented steps to increase CHCS II security. CHCS II eventually will store the records of more than 8.5 million military personnel and their families, allowing doctors to retrieve medical histories on their patients. Defense has approved use of CHCS II at seven military hospitals across the country. The thefts at TriWest are still unsolved.**

Source: http://www.gcn.com/vol1_no1/daily-updates/20816-1.html

Internet Alert Dashboard



Top 10 Target Ports	137 (netbios-ns), 80 (http), 1433 (ms-sql-s), 139 (netbios-ssn), 135 (???), 4662 (???), 3389 (ms-term-serv), 445 (microsoft-ds), 53 (domain), 21 (ftp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

[[Return to top](#)]

General Sector

23. *January 09, Associated Press* — **OAS meeting focuses on security threats.** Officials from throughout the Americas are holding a meeting to discuss concerns that terrorists could use remote islands as stop-off points on their way to carry out attacks. **In a three-day Organization of American States (OAS) meeting that began Wednesday night, officials were considering ways to cooperate in preventing terrorists from operating in the Caribbean or using it as a way-station for attacks on the United States.** "We are on the threshold of the reevaluation of the entire regional security system," OAS Assistant Secretary-General Luigi Einaudi said. **Officials say they are concerned terrorists could pass through small airports or step off boats on poorly patrolled coastlines as they head for their targets. They warn that if terrorists slip into U.S. territories such as Puerto Rico or the U.S. Virgin Islands, the United States is a short plane ride away.** Others argue that the October bombing of a nightclub on the Indonesian island of Bali that killed 192 people suggests Caribbean tourist resorts could be targeted by terrorists. **"The vulnerability for most Caribbean states is in the tourist area," said Anthony Bryan, professor of international relations at the University of Miami's North-South Center. There are few, if any, terrorist groups based in the Caribbean, experts say. But the threat of outsiders taking advantage of what some see as "relaxed" security is of greater concern, said Paul Wilkinson, a professor at the University of St. Andrews in Scotland who studies terrorism.**
Source: <http://www.washingtonpost.com/wp-dyn/articles/A31297-2003Jan9.htm> 1

24. *January 09, Associated Press* — **Pakistani police arrest 3 suspected al Qaeda operatives.** Pakistani police working with the FBI raided a home on the outskirts of Karachi early Thursday, arresting three suspected al Qaeda operatives and several other people after the surrounded fugitives threw grenades and opened fire with automatic weapons, police said. None of the security officials were injured. Officials said they had received a tip about the home and had had it under surveillance for a month. **The identities of the suspects were not immediately released. The two foreign men were believed to be from the Middle East, but their exact nationalities were not clear, Ahmad said.**
Source: http://www.usatoday.com/news/world/2003-01-09-pakistan-arrests_x.htm

25. *January 09, New York Times* — **Singapore warns of threat from radical Islamic groups.** Even if the United States is successful in dismantling al Qaeda, radical Islamic groups in Southeast Asia will be capable of further terrorist acts, like the recent one in Bali, the Singaporean government said today. In a 50 page report on the threat of terrorism in Southeast Asia, the government said that some of these groups were around before al Qaeda, and have local agendas, but their link up with the organization headed by Osama bin Laden, has made them more deadly. **"With their radical agenda and their enhanced skills acquired**

from al Qaeda, these groups, if left unchecked will pose a grave threat to the security of South East Asia for a long time to come," the government said. The group with the closest links to al Qaeda, and therefore potentially the most dangerous, is Jemaah Islamiyah, the report says, underscoring what officials from several countries said in recent interviews. While its members were trained at al Qaeda camps, the organization is capable of acting without any orders from Afghanistan, or wherever else bin Laden and its lieutenants are operating from these days. **In one of the most revealing sections of the report said that many of the men recruited into Jemaah Islamiyah, which is headed by an Indonesian cleric and is believed to have been behind the attack in Bali, were not impoverished or uneducated, but smart and well-employed. The government describes the group's recruitment as "noteworthy" and says recruits are painstakingly pursued over 18 months, with the men seeking religious meaning in their lives.**

Source: http://www.nytimes.com/2003/01/09/international/09CND_SING.html

[[Return to top](#)]

NIPC Products & Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

[NIPC Advisories](#) – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

[NIPC Alerts](#) – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

[NIPC Information Bulletins](#) – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

[NIPC CyberNotes](#) – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:

Melissa Conaty (202-324-0354 or mconaty@fbi.gov)

Kerry J. Butterfield (202-324-1131 or kbutterf@mitre.org)

Distribution Information

NIPC Watch and Warning Unit (202-323-3204 or nipc.watch@fbi.gov)

NIPC Disclaimer

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.

